Table 2: Conventional supervised ML approaches in SDN paradigm

| Reference | Supervised ML approach | Task | Findings |
|---|---|---|---|
| Chen and Yu [101] | NN | Collaborative intrusion prevention | Outperformed [102]. Also it achieved a low overhead due to its parallel and simple computational capabilities. |
| He et al. [103] | NN | Solving weighted controller placement problem | Outperformed decision tree and logistic regression. |
| Alvizu et al. [104] | NN | Off-line prediction of traffic demands in a mobile network operator | Reduced the optimality gap below 0.2% (virtual wavelength path-hourly) and 0.45% (wavelength path-hourly). |
| Abubakar et al. [105] | NN | Intrusion detection | An accuracy of 97.3% using NSL-KDD dataset. |
| Chen-Xiao and Ya-Bin [106] | NN | Load balancing | Compared to [107] and static Round Robin strategy, NN achieved better performance and 19.3% decreasing of network latency. |
| Sabbeh et al. [108] | NN | Predicting the performance of SDN | Achieved low mean squared error (MSE). |
| Bendriss et al. [109,110] | NN | SLA enforcement in SDN and NFV | Showed less robust in compared with LSTM. |
| Mestres et al. [111] | NN | Routing in an overlay network | Mean squared error(MSE) reached 1%. |
| Mihai-Gabriel and Victor-Valeriu [112] | NN + biological danger theory | Mitigating DDoS attacks in SDNs | Proposal without simulated proof of applicability. |
| Kokila et al. [113] | RBF-SVM | DDoS attack detection | An accuracy of 95.11% and false positive rate of 0.01%. |
| Phan et al. [114] | Multiple Linear SVM | DDoS attack detection | Reduction of the consumption of SDN's resources. |
| Wang et al. [115] | RBF-SVM | DDoS attack detection | An accuracy of 97.60%. |
| Boero et al. [116] | RBF-SVM | Malware Detection | A detection rate of 80% for malware 95% for normal traffic. False positive rate of 5.4% for malware 18.5% for normal traffic. |
| Phan et al. [117] | Multiple Linear SVM + SOM | DDoS attack detection | An accuracy of 97.6% and false positive rate of 3.85%. |
| FloodDefender Shang et al. [118] | SVM | DoS attack detection | Attack detection rate of 96% with less than 5% of false-positive rate. |
| FADM Hu et al. [119] | SVM | DDoS attack detection | High detection rate when attack rate is higher than 3000 packets per second. |
| Latah and Toker [120] | RBF-SVM | DoS attack detection | An accuracy of 96.25% with false positive rate of 0.26%. |
| Rego et al. [121] | SVM | Traffic classification | SVM was able to detect critical traffic with an accuracy of 77%. |
| Bouacida et al. [122] | Linear-SVM | Detecting long-term load on SDNs | SVM outperformed k-NN and Naive Bayes. |
| Li et al. [123] | C4.5 | Application identification | An average accuracy of 99%. |
| Pasca et al. [124] | C4.5 | Application identification | An accuracy of 98%. outperformed Naive Bayes, Naive Bayes Kernel Estimation, Bayesian Network and SVM. |
| Le et al. [125] | C4.5 | Intrusion detection and prevention | High precision, recall with low false positive rate. |
| Nagarathna and Shalinie [126] | ID3 | Mitigating host location hijacking attacks on SDN controllers | Less overhead in terms of CPI and memory consumption compared to authentication method. |
| Tariq and Baig [127] | C4.5 | Botnet detection | An accuracy of 80%. |
| Qazi et al. [128] | C5.0 | Fine-grained and scalable application classification | An average accuracy of 94%. |
| Leng et al. [129] | C4.5 | Solving the problem of flow table congestion | High compression with large number of flow entries and reduced the flow matching cost. |
| Nanda et al. [130] | C4.5 | Prediction of potential vulnerable hosts | Outperformed NB and decision table. The best results, however,achieved by bayesian network. |
| Stimpfling et al. [131] | Extensions for DTs | New extensions for DTs for better packet classification and lower memory access | Better packet classification for larger rules, reducing the number of memory access by a factor of 3 , and decreasing the size of data structure 45% over EffiCuts. |
| Tang et al. [132] | Enhanced C4.5 | Detection of elephant flows | Improve the accuracy of C4.5 up to 12%, recall rate 88.3%, false positive rate less than 2.13%. |
| Jain et al. [133] | M5Rules | Prediction of QoS violations | Discover different types of correlations. |
| Van et al. [134] | J48-tree | Intrusion detection on OF switches | An overall accuracy of 93.3% and detection rate of 91.81% with low false alarm rates 0.55%. |
| Wijesinghe et al. [135] | DT | Botnet detection | DT showed better results for detecting P2P Botnets whereas SVM and Bayesian networks showed effectiveness in detecting C&C Botnets. |
| Latah and Toker [136] | Comparing different supervised ML algorithms | SDN-based intrusion detection | DT achieved the best level of accuracy over other supervised ML approaches. However, ensemble methods achieved the best false positive rate. |
| Stadler et al. [137] | RF | Estimating service-level metrics | Outperformed regression tree (RT) in terms of estimation accuracy. However, RF is 3x longer than RT in terms computation time. |
| Song et al. [138] | RF | Intrusion detection | An accuracy of 0.99% on KDD99 |
| Miettinen et al. [139] | RF | Automatic identification and security enforcement for IoT devices | An accuracy of 0.815% and low execution time (<1 ms). |
| Abar et al. [140] | RF | QoE prediction | Outperformed k-NN, NN and DT. |
| Amaral et al. [141] | RF | Traffic classification | RF achieved competitive results with the stochastic gradient boosting and extreme. |
| Zago et al. [142] | RF | Cyber threat detection | Outperformed k-NN, naive bayes and logistic regression. |
| Ajaeiya et al. [143] | RF | Cyber threat detection | Outperformed k-NN, naive bayes, bagged-trees and logistic regression in terms of F1-score. |
| Anand et al. [144] | RF | Detecting compromised controller | Outperformed Naive Bayes, SVM, MLP and AdaBoost. |
| Hussein et al. [145] | RF | Intrusion detection | Outperformed SVM, k-NN, DT, NN and DNN. |
| Su et al. [146] | RF | Botnet detection | An average accuracy of 99.77% |
| Chen et al. [147] | XGBOS | DDoS attack detection | Outperformed RF, GBDT and SVM in terms of accuracy and false positive rate. |
| Choudhury et al. [148] | RF and Gradient boosted regression trees. | Prediction of traffic matrix and performance of optical path. | Outperformed rigde regression, LASSO regression, LASSO with quadratic features, MLP, Guassian process regression, gradiant boosted regression trees. |

able to exactly identify and locate the compromised controller when multiple physical controllers are included.

Hussein et al. [145] designed two architectures for building a general solution to defend and enhance the security of communication networks. The first architecture is distributed extraction, centralized processing, and centralized management. The second one is distributed extraction, distributed processing and centralized management. Then the authors introduced a two-stage detection technique. The first stage includes detecting whether an attack happened or not, whereas the second